REMARKS

The Office Action dated March 29, 2004 has been received and carefully noted. The following remarks are submitted as a full and complete response thereto. Claims 1-33 are currently pending in the application and are respectfully submitted for consideration.

Claims 1-4, 6, 11-13, 15, 16, 18-20, 23, 25-30, and 32 were rejected under 35 U.S.C. 103(a) as being unpatentable over Davis (U.S. Patent No. 5,577,121). The Office Action took the position that it would have been obvious for one of ordinary skill in the art to modify Davis to yield the claimed invention.

Applicants respectfully submit that the cited prior art fails to disclose or suggest the subject matter recited in the presently pending claims. Therefore, the rejection is respectfully traversed and reconsideration is respectfully requested for the following reasons.

Claim 1, upon which claims 2-14 are dependent, recites an apparatus for enabling functionality of a component. The apparatus includes a random number generating module for generating a random number, a hash function module in communication with the random number generating module, a host in communication with the random number generating module, at least one memory in communication with the host, an encryption module in communication with the memory, and a comparing device in communication with the encryption module and the hash function module. The

comparing device compares a first bit string to a second bit string in order to generate a function enable output for the component.

Claim 15, upon which claims 16-24 are dependent, recites a component for selectively enabling a functionality of an electronic device. The component includes a means for generating a random bit string, a hash function module in communication with the means for generating, a means for acquiring a guess passcode in communication with the means for generating, an encryption module in communication with the means for acquiring, and a comparing device in communication with the encryption module and the hash function module. The comparing device has an output for transmitting a functionality enable signal therefrom.

Claim 25, upon which claims 26-33 are dependent, recites a method for enabling functionality of an electronic component. The method includes the steps of generating a random number, calculating a first bit string from the random number, determining a second bit string corresponding to the random number, encrypting the second bit string with a public key to generate a third bit string, comparing the third bit string to the first bit string to determine a match, and outputting a function enable signal in accordance with the comparison.

The prior art has failed to produce enablement methods that are effective against reasonably sophisticated attackers. The claimed invention resolves the limitations of the prior art by providing, in one example, a cryptographic method wherein the secure portions of the method are implemented in electronic or computer products. More

specifically, embodiments of the claimed invention implement cryptographic functions for enabling functionality of electronic/computer related components, wherein the relevant secure key related information is contained within computer hardware in a non-volatile memory device and not within a purely software driven configuration. The claimed invention also provides the ability to conduct secure functionality enablement on electronic/computer related components, wherein a public key for enabling the component is contained onboard and utilized in conjunction with a randomly generated component identifier in order to selectively enable additional functionality of the component.

The cited prior art fails to disclose or suggest the elements of the claims, and therefore fails to provide the advantages discussed above.

Davis discloses a transaction system for integrated circuit cards, and more specifically it discloses a method of conducting a transaction between an integrated circuit (IC) card and a transaction terminal which includes a security module. The method includes establishing communication between the terminal and the IC card and separately generating a session key in the IC card using data stored in the IC card and a code associated with the particular IC card and in the security module using data stored in the security module and the code associated with the particular IC card. The session key generated by the IC card is used to encrypt data using an encryption algorithm to obtain a first result and the session key generated by the security module is used to encrypt the same data using the same encryption algorithm to obtain a second result. The first and

second results are compared and the terminal will conduct the transaction only if the comparison establishes that the first result and the second result are identical.

Applicants respectfully submit that the obviousness rejection with respect to claim 1 is improper on its face. Three criteria must be met in order to establish a prima facie case of obviousness. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference. Second, there must be a reasonable expectation of success. Finally, the prior art reference must teach or suggest all the claim limitations. The Office Action, however, has not indicated any motivation for modifying Davis to yield the claimed invention. The Office Action also failed to indicate what elements are missing from Davis or how it would be modified to cover those missing elements. Thus, for at least this reason, applicants respectfully traverse the rejection.

With respect to claim 1, Davis does not disclose or suggest a host as recited in the presently pending claims. One of the functions of the host in the claimed invention is to determine the identification number associated with the component/network switch through communication with the nonvolatile memory via the interface. Once the host determines the identification number, it then contacts the manufacturer to receive the passcode for the component which the user wishes to enable (Specification, Page 11, lines 9-16). Such a host is not disclosed by Davis, rather Davis discloses a reader/writer processor.

Davis does not disclose an encryption module in communication with at least one memory. In Davis, the encryption function takes place within the security module (Column 13, lines 36-42). According to figure 2 in Davis, however, the security module is only in communication with the reader/writer processor and is not in communication with the memory. Therefore, Davis does not disclose an encryption module in communication with at least one memory.

Davis also does not disclose or suggest a comparing device with a function enable output. Davis discloses that "the result is compared with a derived password which the SVC retrieves from its memory. If the result is identical to the derived password stored in the SVC, the security module and correspondingly the POS terminal are verified and the establishment of a secure session is confirmed to the reader/writer." Thus, Davis does not disclose or suggest a comparing device that outputs a function enable signal. Additionally, claim 1 recites in part a comparing device in communication with an encryption module and a hash function module. The comparison in Davis, however, occurs within the SVC which is only in communication with the reader/writer. Therefore, Davis does not disclose a comparing device in communication with an encryption module and hash function module.

For at least these reasons, applicants submit that Davis fails to disclose or suggest critical and important elements of claim 1 and therefore the rejection of claim 1 is improper.

It is also respectfully submitted that claims 2-14 depend from claim 1 and therefore should be allowed for at least their dependence on claim 1, and for the specific limitations recited therein.

With regard to claim 15, Davis does not disclose all of the elements recited therein. Davis does not disclose a separate hash function module in communication with a means for generating a random bit string. Moreover, Davis does not disclose a guess passcode or a means for acquiring the guess passcode. The guess passcode recited in the current claims does not correspond to the derived password described in Davis (Davis, Column 13, lines 57-60). Davis teaches that the derived password is produced by the security module which retrieves from its memory a control password key and encrypts the SVC serial number with the control password key using the DES algorithm, thereby resulting in a derived password (Davis, Column 13, lines 57-60). Whereas the guess passcode recited in the current claims is transmitted by the manufacturer or other authorized party when the user desires to enable additional functions (Specification, Page 11, lines 3-12). Therefore, the guess passcode is not a password that is derived from a key that is stored in memory as disclosed by Davis, and the prior art does not disclose a means for acquiring a guess passcode.

For at least these reasons, applicants submit that Davis fails to disclose or suggest critical and important elements of claim 15 and thus the rejection of claim 15 is improper.

It is also respectfully submitted that claims 16-24 depend form claim 15 and therefore should be allowed for at least their dependence on claim 15, and for the specific limitations recited therein.

With respect to claim 25, Davis does not disclose or suggest "determining a **second** bit string corresponding to the random number." Nor does Davis disclose or suggest "encrypting the second bit string with a **public key** to generate a third bit string." Instead, Davis discloses encrypting the random number with the security module session key which is maintained exclusively within the memory of the security module (Davis, Column 13, lines 34-42). Additionally, claim 25 recites, in part, the step of "comparing the third bit string to the first bit string to determine a match." Davis, on the other hand, discloses comparing the random number encrypted by the security module to the response certificate from the SVC. Therefore, Davis does not disclose or suggest comparing the third bit string to the first bit string.

For at least these reasons, applicants submit that Davis fails to disclose or suggest critical and important elements of claim 25 and therefore the rejection of claim 25 is improper.

It is also respectfully submitted that claims 26-33 depend from claim 25 and therefore should be allowed for at least their dependence on claim 25, and for the specific limitations recited therein.

Claims 5, 7-10, 17, 21, 22, and 31 were rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Wang (U.S. Patent No. 5,500,808). Applicants

submit that the cited prior art fails to disclose or suggest critical and novel elements of the claims, and therefore the rejection is respectfully traversed.

Wang discloses an apparatus and method for estimating time delays using unmapped combinational logic networks. More specifically, Wang discloses a method for simulating the time delay associated with signal propagation through a mapped and optimized logic network for a selected target technology using only information from an unmapped logic network. The method includes the time delay characteristics of the mapping and optimization strategies used to generate the optimized network from a library of standard gates for the target technology. Wang discloses that the method generates a time delay simulator for the mapped and optimized logic network in the target technology based upon the unmapped logical network.

As discussed above, Davis does not disclose or suggest all of the elements of the presently pending claims. Moreover, Wang fails to cure the deficiencies of Davis. The Office Action relies on Wang for the proposition that "an automated design system first converts Boolean logic equations or a description of a logic circuit in a hardware description language to an unmapped logic network." Despite this disclosure, the combination of Davis and Wang still fails to suggest or disclose the specific configurations recited in claims 5, 7-10, 17, 21, 22, and 31.

Furthermore, it is noted that claims 5 and 7-10 are dependent upon claim 1, claims 17, 21, and 22 are dependent upon claim 15, and claim 31 is dependent upon claim 25. Applicants therefore respectfully submit that claims 5, 7-10, 17, 21, 22, and 31 should be

allowed for at least their dependence on claims 1, 15, and 25, and for the specific limitations recited therein.

Claims 14, 24, and 33 were rejected under 35 U.S.C. 103(a) as being unpatentable over Davis in view of Conley (U.S. Patent No. 6,651,107 B1). Applicants submit that the cited prior art fails to disclose or suggest critical and novel elements of the claims, and therefore the rejection is respectfully traversed.

Conley discloses a reduced hardware network adapter and communication. More specifically, Conley discloses a computer communications system having a transmit buffer coupled to at least one transmit data line. The transmit buffer receives data from a host computer and temporarily stores the data before transmitting the data over the transmit data line to a physical link of a data network. A receive buffer is coupled to at least one receive data line, the receive buffer adapted to receive data from a physical link of a data network over the receive data line and temporarily store the data before providing the data to a computer. Conley further discloses a computer communications system that includes a media access controller including a receive buffer coupled to receive data from a data network and temporarily store the data before providing the data to the host computer.

Davis and Conley, whether taken alone or in combination, do not disclose or suggest the elements of claims 14, 24, and 32. Davis and Conley fail to disclose the use of a network switch **and** a media access controller. Furthermore, it is noted that claim 14, 24, and 32 are dependent upon claims 1, 15, and 25 respectively. Therefore,

applicants respectfully submit that claims 15 and 32 should be allowed for at least their dependence on those claims, and for the limitations recited therein.

For the reasons stated above, Applicants respectfully submit that the cited prior art references fail to disclose or suggest critical and important elements of the claimed invention. These distinctions are more than sufficient to render the claimed invention unobvious. It is therefore requested that all of claims 1-33 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

SIGNATURE ON ORIGINAL

Majid AlBassam
Registration No. 54,749

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

MSA:cct